WHAT IS CLAIMED IS:

1. A method for securing data, said method comprising:
receiving a first password corresponding to a software application;
generating a first mask value based on the first password;
combining the first mask value with a first encryption key, wherein the first encryption key is derived from a generated key and a known value, the combining resulting in a tied key;
receiving a second password corresponding to the software application;
generating a second mask value based on the second password;
separating a recovered encryption key from the tied key using the second mask value, the recovered encryption key including a recovered generated key and a recovered known value; and
encrypting data using the recovered generated key.

2. The method as described in claim 1 further comprising:
encrypting the tied key using a second encryption key, the encrypting resulting in a first encrypted tied key; and
returning the first encrypted tied key to the software application.

3. The method as described in claim 2 further comprising:
receiving a second encrypted tied key; and
combining the second encrypted tied key with the second encryption key, the combining resulting in a recovered tied key.

4. The method as described in claim 2 further comprising:
determining whether a matched encryption tied key is available corresponding to the second encryption key; and
sending the matched encryption tied key to a security module in response to the determination.

5. The method as described in claim 2 further comprising:
determining whether a matched encrypted tied key is available corresponding to the second encryption key; and
sending the first password to a security module in response to the determination.

6. The method as described in claim 1 further comprising:
determining whether the recovered known value is correct; and
processing a data file based on the determination.

7. The method as described in claim 6 wherein the processing is selected from the group consisting of encrypting the data file using the recovered generated key and decrypting the data file using the recovered generated key.

8. An information handling system comprising:
one or more processors;
a memory accessible by the processors;
one or more nonvolatile storage devices accessible by the processors;
a hardware security module accessible by the processors;

a data security tool for securing data using the hardware security module, the data security tool including:

means for receiving a first password corresponding to a software application;

means for generating a first mask value based on the first password using the hardware security module;

means for combining the first mask value with a first encryption key using the hardware security module, wherein the first encryption key is derived from a generated key and a known value, the combining resulting in a tied key;

means for receiving a second password corresponding to the software application;

means for generating a second mask value based on the second password using the hardware security module;

means for separating a recovered encryption key from the tied key using the second mask value, the recovered encryption key including a recovered generated key and a recovered known value; and

means for encrypting data using the recovered generated key.

9. The information handling system as described in claim 8 further comprising:

means for encrypting the tied key using a second encryption key, the encrypting resulting in a first encrypted tied key; and

means for returning the first encrypted tied key to the software application.

10. The information handling system as described in claim 9 further comprising:

means for receiving a second encrypted tied key; and

means for combining the second encrypted tied key with the second encryption key using the hardware security module, the combining resulting in a recovered tied key.

11. The information handling system as described in claim 9 further comprising:

means for determining whether a matched encryption tied key is available corresponding to the second encryption key; and

means for sending the matched encryption tied key to the hardware security module in response to the determination.

12. The information handling system as described in claim 8 further comprising:

means for determining whether the recovered known value is correct; and

means for processing a data file corresponding to the determination.

13. The information handling system as described in claim 12 wherein the means for processing is selected from the group consisting of a means for encrypting the data file using the recovered generated key and a means for decrypting the data file using the recovered generated key.

14. A computer program product stored in a computer operable media for securing data, said computer program product comprising:
means for receiving a first password corresponding to a software application;
means for generating a first mask value based on the first password;
means for combining the first mask value with a first encryption key, wherein the first encryption key is derived from a generated key and a known value, the combining resulting in a tied key;
means for receiving a second password corresponding to the software application;
means for generating a second mask value based on the second password;
means for separating a recovered encryption key from the tied key using the second mask value, the recovered encryption key including a recovered generated key and a recovered known value; and
means for encrypting data using the recovered generated key.

15. The computer program product as described in claim 14 further comprising:
means for encrypting the tied key using a second encryption key, the encrypting resulting in a first encrypted tied key; and
means for returning the first encrypted tied key to the software application.

16. The computer program product as described in claim 15 further comprising:

means for receiving a second encrypted tied key; and
means for combining the second encrypted tied key with the second encryption key, the combining resulting in a recovered tied key.

17. The computer program product as described in claim 15 further comprising:
means for determining whether a matched encryption tied key is available corresponding to the second encryption key; and
means for sending the matched encryption tied key to a security module in response to the determination.

18. The computer program product as described in claim 15 further comprising:
means for determining whether a matched encrypted tied key is available corresponding to the second encryption key; and
means for sending the first password to a security module in response to the determination.

19. The computer program product as described in claim 14 further comprising:
means for determining whether the recovered known value is correct; and
means for processing a data file corresponding to the determination.

20. The computer program product as described in claim 19 wherein the means for processing is selected from the group consisting of a means for encrypting the data file using the recovered generated key and a means for

decrypting the data file using the recovered generated key.